CONFIDENTIAL

5 June 85

MEMORANDUM FOR THE ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE)

SUBJECT: The Director of Central Intelligence SAFEGUARDS Supplement to DCID 1/16 (U)

Reference: ASD/C^{3}I Memorandum dated 10 May 1985, Subject: Defense Central Intelligence Memorandum NFIC-9.11/1, dated 22 January 1985.

1. (C) As you are aware, the SAFEGUARDS were developed under the DCI COMPUSEC program to evaluate the vulnerabilities of thirteen Critical Systems, seven of which are under my cognizance as the approving authority. DIA has evaluated the seven Critical Systems using the SAFEGUARDS as a guideline and has found them to be useful in documenting system vulnerabilities.

2. (U) It is our view that the documents are aimed at different purposes. The DoD CRITERIA are aimed at describing to vendors and system acquisition authorities the features necessary to achieve certifiable levels of security in the automated system, while the SAFEGUARDS are intended as interim guidelines for accreditation of operational intelligence systems and in particular the Critical Systems, processing SCI, identified by the DCI. Both documents can be further enhanced to address technical discrepancies but should not be viewed as incompatible even though there are some technical inconsistencies.

3. (U) As requested in your memorandum, DIA has compared the CRITERIA with the SAFEGUARDS, and has assessed the impact of their implementation within the DoD for systems for which I am the accreditation authority. The general conclusions drawn from that assessment are: first, the SAFEGUARDS and the CRITERIA are not consistent in the area of assurance, and in implementation philosophy; second, the SAFEGUARDS, as an accreditation document, and the CRITERIA, as a certification document, could be used together to achieve a continuous program of enhanced ADP security as technology evolves. The technical assessment is at the enclosure.

4. (U) To achieve an orderly transition of systems to a more secure base, I recommend we establish a group to develop a common set of security criteria through the NTISSC process. For that purpose, I fully support the 28 January 1985 Secretary of Defense direction to DIRNSA to establish a working group to develop a common set of security criteria for use by all Designated Approving Authorities.

Signed

DIA review completed.

25X1

Acting Director

1 Enclosure a/s

Coordination Cy
RS-A R/F Cy
RS R/F Cy
RSE-4 R/F Cy
RSE R/F Cy
RSI R/F Cy
Director's Cy

Classified By: DIA/RSE

DIA ASSESSMENT

1. The referenced memorandum requests that DIA review the DCI SAFEGUARDS document for consistency with the DoD Computer Security Evaluation Center's Criteria (a.k.a. The CRITERIA), and for impact of implementation of the SAFEGUARDS within the DoD. The version of the SAFEGUARDS being used is dated December 1984, of the CRITERIA, August 1983.

Consistency

2. Comparing the preface of the CRITERIA with the foreword of the SAFEGUARDS one notes a difference in intent between the documents. In particular, the SAFEGUARDS are intended to apply to some 13 operational "Critical Systems" as an interim accreditation measure to improve the security posture of those particular systems. These Critical Systems were designed, developed, and implemented prior to the existence of the CRITERIA. The CRITERIA is intended to describe to vendors and acquisition personnel the security features deemed necessary in order to achieve identifiable and certifiable levels of security protection. In respect to intent the documents are incomparable rather than inconsistent.

3. On the other hand, both documents address specific feature requirements for system security. It would seem desirable that these features, which must clearly differ in implementation, should be stated consistently. In this regard both the DoD and the DCI are indeed fortunate in that the primary author of the CRITERIA [redacted] is also a primary author of the SAFEGUARDS, and that under her guidance the features for the compartmented mode in the SAFEGUARDS were chosen to match the B2 level of the CRITERIA, thus making comparison for consistency feasible. 25X1

Comparison of Class B2 with the Compartmented Mode

4. Assurance. The implementation of features will differ because of the difference in intent between the CRITERIA and the SAFEGUARDS. In particular the way in which assurance is achieved is different. Assurance is a combination of trust in procedure and personnel, and of trust in the correctness of automation. The CRITERIA places more assurance requirements against the correctness of automation of features and less against the people and environment, whereas the SAFEGUARDS places less assurance requirements against the correctness of automation and more against people and environment. This tradeoff is a reasonable course of action for the SAFEGUARDS in order that it might accomplish the objective of dealing with currently operational critical systems. Thus the assurance features of the CRITERIA and the SAFEGUARDS could be called consistent in net effect.

5. Discretionary Access Control. A difference exists in that the CRITERIA allows granting of discretionary access permission to an arbitrary user by some other arbitrary user, whereas the SAFEGUARDS allow only a cognizant authority to extend access permissions against classified information.

Enclosure to C-10,048/RSE

It is interesting that DoD policy (DoD 5200.28-M), DCI policy (DCID 1/16), and the Control permission of the [redacted] all match more closely the SAFEGUARDS version of Discretionary Access Control than the version given in the CRITERIA. The SAFEGUARDS and the CRITERIA are inconsistent, with the SAFEGUARDS apparently offering the more secure approach. 25X1

6. Mandatory Access Control. The CRITERIA and the SAFEGUARDS use different words in the statement of this requirement. Both statements imply a no write down property and both permit arbitrary creation and classification of data.

DIA has noted the provision for arbitrary creation and classification of data in both documents as it transgresses the requirement for a classification authority to determine the classification of data.

7. Object Reuse, Audit, and Trusted Path. These requirements are basically consistent.

8. Identification and Authentication. Here there is a major inconsistency as the CRITERIA requires protection of authentication information, while the SAFEGUARDS do not. The CRITERIA has the correct requirement as unprotected information of this sort poses a security vulnerability.

9. Labels, System Architecture, System Integrity. These features are addressed by both documents but their statements are not comparable. The lack of comparability arises out of the difference in intent between the documents. While the CRITERIA calls for a great deal of robustness in these features, the SAFEGUARDS recognizes the lack of feasibility of implementation of such robustness in existing (older) systems without recourse to system replacement.

10. Trusted Facility Management, Trusted Recovery, and Environmental and Administrative Protections. These requirements are not comparable between the documents. In general, the CRITERIA places less of its assurance in these non-automated functions than does the SAFEGUARDS.

11. Testing, and Design Specification and Verification. These criteria are incomparable between the documents. In general, the CRITERIA places more of its assurance in these automated functions than does the SAFEGUARDS.

12. Covert Channel Analysis. This assurance requirement is not addressed in the SAFEGUARDS but is addressed in the CRITERIA. There is a significant technological problem involved in performing such an analysis on a critical system due to the lack of structure inherent in its operating system. At the B2 level, and above, of the CRITERIA, such an analysis is made feasible because of the intense structuring of the operating system. Such structuring is not inherent in the Critical Systems.

13. Trusted Distribution is not addressed in the CRITERIA at the B2 level. The CRITERIA places similar assurances in automated elements of the system rather than in this administrative element.

Impact

14. The impact on DIA mission of implementation of the SAFEGUARDS would be in the area of resource expenditure and ability to respond to operational security problems of the Critical Systems. DIA has found that the SAFEGUARDS do not address several of the vulnerabilities which have been identified in the Critical Systems. Therefore, it is our conclusion that while improvement of the security posture of the "Critical Systems" will be achieved through implementation of the SAFEGUARDS (increased auditing, stronger user identification, increased labeling responsibility, etc.), some of the real operational vulnerabilities of these systems will be incompletely and inadequately addressed (uncontrolled asynchronous interfaces, data integrity, channel reliability, etc.)

15. DIA has not concurred with implementation of the SAFEGUARDS as large resource expenditures would be required in order to comply with it, and those resources have not been available. DIA cannot fully implement the SAFEGUARDS until the resources required to comply with them are made available. DIA has, within resources available, identified the highest priority vulnerabilities in its Critical Systems and is attempting to correct them.

Conclusion and Recommendation

16. DIA believes that the SAFEGUARDS, as an accreditation document, and the CRITERIA, as a certification document, are each of value, and that, with great care, they could be used together to achieve a continuous transitional program of enhanced ADP security for the Intelligence Community and the DoD. For this reason, the DIA staff recommends that a carefully conceived uniform accreditation policy be developed for use by all Designated Approving Authorities. Such a policy should incorporate the excellent ideas represented in the CRITERIA and in the SAFEGUARDS.